

ABSTRACT OF THE DISCLOSURE

5 Because the additional hardware required to support security functions is a relatively small fraction of the overall device hardware, this type of SPU can be competitive with ordinary non-secure CPUs or microcontrollers that perform the same functions. A set of minimal initialization and management hardware and software is added to, e.g., a standard CPU/microcontroller. The additional hardware and/or software creates an SPU environment and performs the functions
10 needed to virtualize the SPU's hardware resources so that they can be shared between security functions and other functions performed by the same CPU.

1. The first of these is the fact that the
2. second of these is the fact that the
3. third of these is the fact that the
4. fourth of these is the fact that the
5. fifth of these is the fact that the
6. sixth of these is the fact that the
7. seventh of these is the fact that the
8. eighth of these is the fact that the
9. ninth of these is the fact that the
10. tenth of these is the fact that the

**FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L. L. P.**
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-6600